STATE OF ALABAMA

Information Technology Baseline

Baseline 660-02B1: Server Security – Windows Server 2003

1. INTRODUCTION:

Though operating system vendors have taken steps to make their operating system baseline configurations more secure on a default installation, additional operating system hardening efforts are usually required to enhance the confidentiality, integrity, and availability of the data present on the servers and accountability in regards to persons authorized access to the servers as well as complete restriction of unauthorized access. Furthermore, dependent on server functionality (e.g., domain controllers or Web servers) additional hardening must be considered based on the server's level of exposure to cyber threats. In order to reduce the exposure of State of Alabama server-based computing resources to cyber-related threats and unauthorized access, secure operating system baseline configurations are necessary as a fundamental countermeasure.

2. OBJECTIVE:

Define standard configuration settings for a secure operating system computing baseline for State of Alabama server computing resources.

3. SCOPE:

These requirements apply to all State of Alabama servers utilizing the Windows Server 2003 operating system.

4. REQUIREMENTS:

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) recommend that Windows 2003 servers be configured in accordance with the guidelines published by Microsoft Corporation. The Windows Server 2003 Security Guide provides the baseline configuration to be implemented on all State of Alabama servers running the Windows Server 2003 operating system.

Download the Windows Server 2003 Security Guide from the Microsoft Download Center:
http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

To determine the specific security settings to use, organizations will first need to determine the server's role (domain controller, file server, Web server, etc.) and the appropriate operating environment (Legacy Client, Enterprise Client, or Specialized Security – Limited Functionality (SSLF)) based on the client types supported and/or the need for tighter security.

Document the designated operating environment and server role in system security plans and local operating procedures.

Ensure secure system configurations by routinely and proactively updating systems with fixes, patches, definitions, and service packs in accordance with the requirements of State IT Standard 670-03S1: Vulnerability Management and organizational vulnerability management program(s).

5. DEFINITIONS:

ENTERPRISE CLIENT: Environment consisting of an Active Directory® domain with member servers and domain controllers that run Windows Server 2003 and client computers that run Windows 2000 and Windows XP.

LEGACY CLIENT: Environment consisting of an Active Directory® directory service domain with member servers and domain controllers that run Windows Server 2003 and some client computers that run Microsoft Windows 98 and Windows NT® 4.0. Computers running Windows 98 must have the Active Directory Client Extension (DSCLient) installed.

SSLF: The SSLF environment consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003 and clients that run Windows 2000 and Windows XP. The SSLF security settings in Microsoft's "Windows Server 2003 Security Guide" track closely with the security level historically represented in the guidelines offered by NSA, NIST, and the security community. However, the SSLF settings are so restrictive that many applications may not function. This may affect server performance and make it more of a challenge to manage the servers. Also, client computers that are not secured by the SSLF policies could experience communication problems with client computers and servers that are secured by the SSLF policies.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 670-03S1: Vulnerability Management

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	12/18/2007	